UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,720	08/31/2001	Suresh N. Chari	YOR920010711US2	1361

7590 06/06/2005

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/943,720	CHARI ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *19-28,31-35,49-51,54 and 57* is/are allowed.

6)☒ Claim(s) *1-4,10-13,15,18,29,30,36-43,52,53,55 and 56* is/are rejected.

7)☒ Claim(s) *5-10,14,16-18, and 44-48* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *see attached*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on August 31, 2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. The disclosure is objected to because of the following informalities: On page 1, line 10, application 09/240,503 is cross referenced and the status of the application should be updated to indicate that the application is now abandoned.

Appropriate correction is required.

Claim Objections

3. Claims 10 are 18 are objected to because of the following informalities: On line 1, it is recited of "at least one table" that is a lack of antecedent basis. It is unclear from the claim if the "table" is a "lookup table" or a "randomized table" as is claimed in claim 1. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4,10-13,15,18,29,30,36-43,52,53,55, and 56 are rejected under 35 U.S.C. 102(b) as being anticipated by Chari et al, entitled "Towards Sound Approaches to Counteract Power-Analysis Attacks".

As per claim 1, Chari et al discloses of a method comprising providing a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see page 404, section 3.3).

As per claim 2, it is taught by Chari et al of using one randomized table (see page 404, section 3.3).

As per claim 3, it is disclosed by Chari et al of obtaining data processing operations (see page 404, section 3.3).

As per claim 4, Chari et al discloses of creating a randomized table includes applying a Table Split operation to at least one of said lookup tables resulting in split lookup tables (see page 404, section 3.3).

As per claim 10, Chari et al teaches of the table is a table from a COMP128 application (see abstract and page 404, section 3.3).

As per claim 11, it is disclosed by Chari et al of the number of elements in the lookup table is given by a power of two (see page 404, section 3.3).

As per claim 12, Chari et al teaches of employing said at least one randomized table in a cryptographic process, applying said at least one randomized table for securely handling information in said cryptographic process (see page 404, section 3.3).

As per claim 13, Chari et al discloses of prior to performing said cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information, performing the cryptographic process on the transformed information involving the use of said randomized table, and retransforming the transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see page 404, section 3.3).

As per claim 15, Chari et al teaches of employing data processing operation as a countermeasure against a first order side channel attack (see page 405, section 3.4).

As per claim 18, it is disclosed by Chari et al that a table is a table from an application of General Countermeasures Against Side-Channel Attacks (see page 405, section 3.4).

As per claim 29, it is disclosed by Chari et al of that the number of elements in the lookup table is 200 (see page 404, section 3.3).

As per claim 30, Chari et al discloses of an article of manufacture comprising computer readable program code embodied thereon for causing resistance to side channel attacks that provides a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see abstract; page 404, section 3.3; page 405, section 3.4).

As per claim 36, Chari et al teaches of a method comprising providing a data processing operation involving a first lookup table in a cryptographic process, said lookup table having a first lookup table size, creating a randomized table in which entries or indices are statistically independent of entries or indices of said first lookup table, said randomized table having a randomized table size being smaller than said first lookup table size, employing said randomized table for securely handling information in said cryptographic process prior to performing the cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information, performing the cryptographic process on the transformed information involving the use of said randomized table, and retransforming the

transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see page 404, section 3.3 and page 405, section 3.4).

As per claim 37, it is taught by Chari et al of using one randomized table (see page 404, section 3.3).

As per claim 38, it is disclosed by Chari et al of the cryptographic process is performed in a cryptographic information processing system (see abstract).

As per claim 39, Chari et al discloses a chip card comprising a module for providing a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see section 1, page 398 and page 404, section 3.3).

As per claim 40, Chari et al teaches of a fixed lookup table (page 404, section 3.3).

As per claim 41, it is disclosed by Chari et al of an apparatus for a randomizer module to create at least one randomized table in which entries and/or indices are statistically independent of entries; and/or indices of any table from a provided set of

lookup tables, each individual table from said at least one randomized table having a randomized table size, wherein: a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all said at least one lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables; and a processing module to perform said data processing operation employing said first randomized table (page 404, section 3.3).

As per claim 42, Chari et al teaches that the randomized module forms the provided set of lookup tables (see page 404, section 3.3).

As per claim 43, it is taught by Chari et al that the randomizer module includes a splitting module to perform a table split operation upon the subset of the set of lookup tables resulting in split lookup tables (see page 404, section 3.3).

As per claim 52, Chari et al discloses of an article of manufacture comprising computer readable program code embodied thereon for causing resistance to side channel attacks that provides a data processing operation involving a first lookup table in a cryptographic process, said lookup table having a first lookup table size, creating a randomized table in which entries or indices are statistically independent of entries or indices of said first lookup table, said randomized table having a randomized table size being smaller than said first lookup table size, employing said randomized table for securely handling information in said cryptographic process prior to performing the cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information, performing the

cryptographic process on the transformed information involving the use of said randomized table, and retransforming the transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see abstract; page 404, section 3.3 and page 405, section 3.4).

As per claim 53, Chari et al discloses of a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for causing resistance to side channel attacks that provides a data processing operation involving at least one lookup table, each particular table from said at least one lookup table having a particular lookup table size and a particular lookup table index size and creating at least one randomized table in which entries and/or indices are statistically independent from entries and/or indices of said at least one lookup table, each individual table from said at least one randomized table having a randomized table size, wherein a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables (see abstract; page 404, section 3.3; page 405, section 3.4).

As per claim 55, Chari et al teaches of a program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for causing resistance to side channel attacks that provides a data processing operation involving a first lookup table in a cryptographic process, said lookup table having a first lookup table size, creating a randomized table in which entries or indices are statistically

independent of entries or indices of said first lookup table, said randomized table having a randomized table size being smaller than said first lookup table size, employing said randomized table for securely handling information in said cryptographic process prior to performing the cryptographic process, transforming the information by applying a secret-sharing operation to the elements of the information where each element of the information is related to multiple elements of the transformed information, performing the cryptographic process on the transformed information involving the use of said randomized table, and retransforming the transformed and cryptographically processed information by applying an inverse secret-sharing operation to the transformed and cryptographically processed information (see abstract; page 404, section 3.3; and page 405, section 3.4).

As per claim 56, it is disclosed by Chari et al of a computer program product comprising a computer useable medium having computer readable program code embodied thereon for causing resistance to side channel attacks that provides a randomizer module to create at least one randomized table in which entries and/or indices are statistically independent of entries; and/or indices of any table from a provided set of lookup tables, each individual table from said at least one randomized table having a randomized table size, wherein: a first sum of sizes of all said randomized tables is smaller than a second sum of sizes of all said at least one lookup tables, or the maximum index size of said randomized tables is less than the maximum index size of the lookup tables; and a processing module to perform said data

processing operation employing said first randomized table (see abstract; page 404, section 3.3; and page 405, section 3.4).

Allowable Subject Matter

6. Claims 5-9,14,16,17, and 44-48 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

7. Claims 19-28,31-35,49-51,54, and 57 are allowed.

8. The following is a statement of reasons for the indication of allowable subject matter:

It was not found to be taught in the prior art of performing a table split operation on a lookup table to form a collection of split tables, performing a table mask operation on the collection of split tables, performing a table aggregate operation on at least two of the plurality of masked tables, and performing data processing operations on a combination of the split, masked, aggregate, and lookup tables.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kocher et al, US 2001/0053220 discloses of preventing differential power analysis attacks.

Kocher et al, US 2001/0002486 discloses of preventing leakage in cryptographic processing systems.

Benoit, U.S. Patent 6,820,814 discloses of countermeasures using secret key algorithms.

Singer, U.S. Patent 6,724,894 discloses of reducing vulnerability to side channel attacks.

Patarin et al, U.S. Patent 6,658,569 discloses of protecting against physical attacks by using secret keys.

Kocher et al, U.S. Patent 6,381,699 discloses of discloses of preventing leakage in cryptographic processing systems.

Kocher et al, U.S. Patent 6,304,658 discloses of preventing leakage in cryptographic processing systems.

Messerges et al, U.S. Patent 6,295,606 discloses of preventing leakage in cryptographic processing systems.

Kocher et al, U.S. Patent 6,278,783 discloses of minimization of leakage for smart cards to improve cryptographic protocols.

Kocher et al, "Differential Power Analysis" discloses of preventing leakage in cryptographic processing systems.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

CR
May 26, 2005

5/26/05